This Page Is Inserted by IFW Operations
and is not a part of the Official Record

# BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.**

**PCT** WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04L 12/22, 29/06, 9/32

A1

(11) Internationale Veröffentlichungsnummer: **WO 99/21324**

(43) Internationales Veröffentlichungsdatum: 29. April 1999 (29.04.99)

(21) Internationales Aktenzeichen: PCT/EP98/06211

(22) Internationales Anmeldedatum: 30. September 1998 (30.09.98)

(30) Prioritätsdaten:
97118146.6 20. Oktober 1997 (20.10.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: DEININGER, Andreas [DE/DE]; Fuchsbergstrasse 6, D–86938 Schondorf (DE). LAUER, Maria [DE/DE]; Ludwig–Weiß–Strasse 45, D–82275 Emmering (DE). MÜLLER, Klaus–Dieter [DE/DE]; Wilbrechtstrasse 85, D–81477 München (DE). NAUER, Bernhard [DE/DE]; Fuggerstrasse 4, D–81373 München (DE).

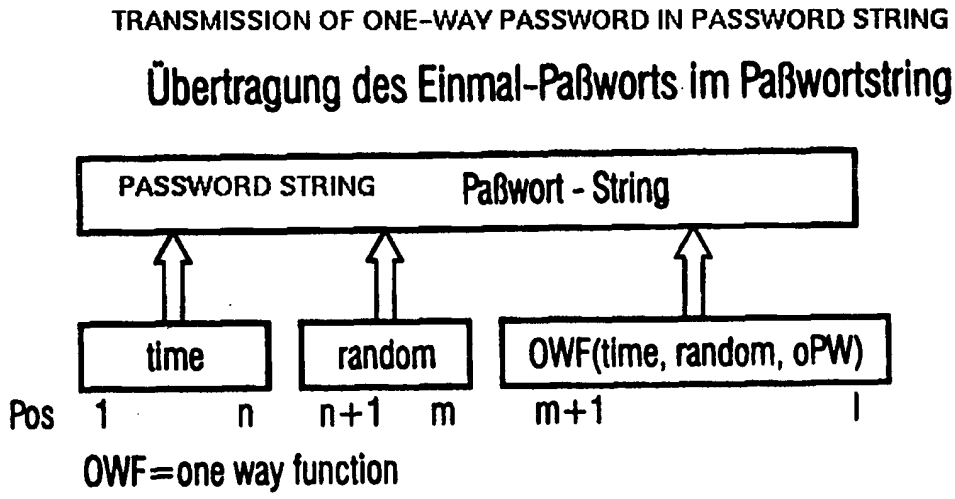
(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) Bestimmungsstaaten: CN, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
*Mit internationalem Recherchenbericht.*
*Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.*

(54) Title: METHOD FOR SECURING ACCESS TO AN APPLICATION OF A NETWORKED SYSTEM

(54) Bezeichnung: VERFAHREN ZUR SICHERUNG DES ZUGANGS ZU EINER ANWENDUNG EINES VERNETZTEN SYSTEMS




(57) Abstract

Some distributed applications are still based on a communications protocol which only provides for the transmission of an unstructured password string in terms of protecting access. According to the inventive method, a structured one–way password is mapped into the unstructured password string with a communications protocol of this type, resulting in better access security.

**(57) Zusammenfassung**

Manchen verteilten Anwendungen liegt noch ein Kommunikations–Protokoll zugrunde, das bezüglich der Sicherung des Zugangs nur die Übertragung eines unstrukturierten Paßwort–Strings vorsieht. Durch das erfindungsgemäße Verfahren wird bei einem solchen Kommunikations–Protokoll in den unstrukturierten Paßwort–String ein strukturiertes Einmal–Paßwort abgebildet und dadurch die Zugangssicherheit entsprechend erhöht.

*LEDIGLICH ZUR INFORMATION*

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **AL** | Albanien | **ES** | Spanien | **LS** | Lesotho | **SI** | Slowenien |
| **AM** | Armenien | **FI** | Finnland | **LT** | Litauen | **SK** | Slowakei |
| **AT** | Österreich | **FR** | Frankreich | **LU** | Luxemburg | **SN** | Senegal |
| **AU** | Australien | **GA** | Gabun | **LV** | Lettland | **SZ** | Swasiland |
| **AZ** | Aserbaidschan | **GB** | Vereinigtes Königreich | **MC** | Monaco | **TD** | Tschad |
| **BA** | Bosnien-Herzegowina | **GE** | Georgien | **MD** | Republik Moldau | **TG** | Togo |
| **BB** | Barbados | **GH** | Ghana | **MG** | Madagaskar | **TJ** | Tadschikistan |
| **BE** | Belgien | **GN** | Guinea | **MK** | Die ehemalige jugoslawische Republik Mazedonien | **TM** | Turkmenistan |
| **BF** | Burkina Faso | **GR** | Griechenland | | | **TR** | Türkei |
| **BG** | Bulgarien | **HU** | Ungarn | **ML** | Mali | **TT** | Trinidad und Tobago |
| **BJ** | Benin | **IE** | Irland | **MN** | Mongolei | **UA** | Ukraine |
| **BR** | Brasilien | **IL** | Israel | **MR** | Mauretanien | **UG** | Uganda |
| **BY** | Belarus | **IS** | Island | **MW** | Malawi | **US** | Vereinigte Staaten von Amerika |
| **CA** | Kanada | **IT** | Italien | **MX** | Mexiko | | |
| **CF** | Zentralafrikanische Republik | **JP** | Japan | **NE** | Niger | **UZ** | Usbekistan |
| **CG** | Kongo | **KE** | Kenia | **NL** | Niederlande | **VN** | Vietnam |
| **CH** | Schweiz | **KG** | Kirgisistan | **NO** | Norwegen | **YU** | Jugoslawien |
| **CI** | Côte d'Ivoire | **KP** | Demokratische Volksrepublik Korea | **NZ** | Neuseeland | **ZW** | Zimbabwe |
| **CM** | Kamerun | | | **PL** | Polen | | |
| **CN** | China | **KR** | Republik Korea | **PT** | Portugal | | |
| **CU** | Kuba | **KZ** | Kasachstan | **RO** | Rumänien | | |
| **CZ** | Tschechische Republik | **LC** | St. Lucia | **RU** | Russische Föderation | | |
| **DE** | Deutschland | **LI** | Liechtenstein | **SD** | Sudan | | |
| **DK** | Dänemark | **LK** | Sri Lanka | **SE** | Schweden | | |
| **EE** | Estland | **LR** | Liberia | **SG** | Singapur | | |

Beschreibung

Verfahren zur Sicherung des Zugangs zu einer Anwendung eines vernetzten Systems

Zur Gewährleistung der Integrität und Schutz vor Mißbrauch sind bei vernetzten Systemen adäquate Schutzmechanismen zwingend erforderlich und vielfach gesetzlich vorgeschrieben. Für offene Systeme sind entsprechende Sicherheitsmaßnahmen in der ITU rec. X.800: „Security Architecture for Open Systems Interconnection" und folgende aufgeführt. Als eine wesentliche Sicherheitsfunktion ist bei jedem Verbindungsaufbau zu einer Komponente (z.B. Rechner, Server) eines vernetzten Systems eine Identifizierung (Identification) und Authentisierung (Authentication) des entfernten Partners, der einen Systemzugang anstrebt, erforderlich.

Im folgenden wird als Beispiel eines vernetzten Systems ein TMN-System (TMN = Telecommunications Management Networks = Netz zur Administration von Telecommunications Anlagen) näher betrachtet. In einem TMN-System existieren u.a. folgende Kommunikationsprotokolle:

a) MML-Protokoll, das den TMN-Zugang über unterschiedliche - oftmals nicht normierte - Schnittstellen unterstützt.
b) Q3-Protokoll, das den TMN-Zugang gemäß ITU rec. X.711 (Common Management Information Protocol) unterstützt.
c) Filetransfer-Protokolle (FTAM, FTP), die den TMN-Zugang gemäß FTAM (ISO 8571) / FTP (RFC 959 u. RFC 1123) unterstützen.

Bei (verteilten) Anwendungen des TMN-Systems, die die genannten Protokolle verwenden, werden derzeit folgende Authentisierungs-Verfahren (peer entity authentication) durchgeführt:

bei a):
Die Authentisierung erfolgt bei einer MML-Anwendung über eine Userid, die im System administriert ist und ein Paßwort, das der User vergibt. Userid und Paßwort werden „unverschlüsselt" über die Leitung übertragen und können abgehört werden; mit dieser Information ist ein unberechtigter Zugriff durch einen Dritten möglich (Replay Attacke).

bei b):
Der Verbindungsaufbau erfolgt bei einer Q3-Anwendung (CMIP-Anwendung) nach dem ACSE Protokoll (ITU rec. X.217); hierbei können Authentisierungsdaten strukturiert (eine entsprechende Syntax ist in ITU rec. X.511 definiert) übertragen werden. Für die Authentisierung kann ein "Replay Protected Password" Mechanismus gem. ITU rec. X.509 (Directory Access Protocol) eingesetzt werden, der durch Verwendung von Einmal-Paßwörtern einen unberechtigten Systemzugang mit einem ausgespähten Paßwort verhindert. Das übertragene Paßwort wird mit Hilfe einer speziellen Einweg-Funktion ("one way function"), für die keine reverse Funktion zur Entschlüsselung existiert, verschlüsselt - d.h. selbst mit Kenntnis der Einweg-Funktion und des einwegverschlüsselten Paßworts ist es nicht möglich, das ursprünglich Paßwort zu rekonstruieren.

Bezüglich der Authentisierung werden hierzu folgende Informationen übertragen:

- Die Initiator Id (Eindeutige Kennung für den entfernten Initiator des Verbindungsaufbaus ).
- Datum/Uhrzeit (time) und/oder Zufallszahl (random), die der Initiator vergibt.
- Ein Einmal-Paßwort (rpPaßwort), das mit Hilfe von Einweg-Funktionen (OWF) aus dem Orginal-Paßwort (oPaßwort), Uhrzeit und/oder Zufallszahl in einer ein- oder zweistufigen Verschlüsselung gebildet wird (vgl. ITU rec. X.509):

Das Orginal-Paßwort ist nur beim Initiator und beim Zielrechner bekannt und kann auf der Leitung nicht abgehört werden. Mit Hilfe der übertragenen Zeit(en) und/oder Zufallszahl(en) wird beim Empfänger die gleiche Verschlüsselung nochmals durchgeführt. Nur bei Übereinstimmung mit dem übertragenen Einmal-Paßwort ist die Authentisierung erfolgreich. Ein Zugangsversuch mit einem abgehörten rpPaßwort ist nicht möglich, da die Authentisierung abgelehnt wird, wenn die Zufallszahl wiederholt wird und/oder die Zeit nicht mehr gültig ist.

bei c):
Bei der Anwendung „Filetransfer" sehen die verwendeten Protokolle FTAM oder FTP beim Verbindungsaufbau eine Zugangssicherung (Identifizierung und Authentisierung) mit Hilfe eines Initiators Id und eines Paßworts vor, wobei das Paßwort als unstrukturierter Text-String (FTP) bzw. Text- oder Binär-String (FTAM) übertragen wird. Durch das Ausspähen der Zugangssicherungs-Daten sind daher Replay Attacken möglich.

In einem TMN-System sind insbesondere die Systemzugänge gemäß b) und c) von Bedeutung. Es ist daher ein einheitlicher Zugangsschutz für Q3 und Filetransfer unter folgenden Randbedingungen erstrebenswert:

- Schutz vor Replay-Attacken auch bei Filetransfer.
- Die Filetransfer-Protokolle für FTAM und FTP sind genormt, eine Protokoll-Änderung - zur Übertragung der Authentisierungsdaten - ist nicht möglich.
- Es soll ein vergleichbar „einfaches" Verfahren, ohne Einsatz von externer Hardwarekomponenten (z.B. Security Box) zum Einsatz kommen.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zur Sicherung des Zugangs zu einem Anwendersystem anzugeben, durch das die Sicherung trotz eines Kommunikations-Protokolls, das bezüglich der Sicherung des Zugangs nur die Über-

tragung eines unstrukturierten Paßwort-Strings vorsieht, erhöht wird.

Diese Aufgabe wird durch ein Verfahren gemäß Anspruch 1 gelöst.

Der Erfindung liegt des weiteren die Aufgabe zugrunde, ein Anwendersystem anzugeben, bei dem die Zugangssicherung trotz eines Kommunikations-Protokolls, das bezüglich der Sicherung des Zugangs nur die Übertragung eines unstrukturierten Paßwort-Strings vorsieht, erhöht ist.

Diese Aufgabe wird durch ein Anwendersystem gemäß Anspruch 6 gelöst.

Durch die erfindungsgemäße Abbildung der strukturierten Information auf einen unstrukturierten Paßwort-String wird ein wesentlich besserer Zugangsschutz ohne Änderung des Übertragungsprotokolls ermöglicht. Der Aufwand für die zusätzlichen Komponenten des Anwendersystems zur Einweg-Verschlüsselung und Validierung ist relativ gering.

Im folgenden wird ein Ausführungsbeispiel der Erfindung anhand der Zeichnung näher erläutert.

FIG 1 zeigt die Generierung der Komponente rpPaßwort eines Einmal-Paßworts nach ITU rec. X.509.

FIG 2 zeigt die Übertragung des Einmal-Paßworts im Paßwortstring.

FIG 3 zeigt die FTAM-/FTP Authentisierung mit Replay Protected Password.

Als Beispiel dient wiederum ein TMN-System. In einem TMN-System ist, wie bereits erwähnt, ein einheitlicher Zugangs-

schutz für die Anwendersysteme „Q3" und „Filetransfer" unter folgenden Randbedingungen erstrebenswert:

- Schutz vor Replay-Attacken auch bei Filetransfer.
- Die Filetransfer-Protokolle für FTAM und FTP sind genormt, eine Protokoll-Änderung - zur Übertragung der Authentisierungsdaten - ist nicht möglich.
- Es soll ein vergleichbar „einfaches" Verfahren, ohne Einsatz von externer Hardwarekomponenten (z.B. Security Box) zum Einsatz kommen.

Die genannten Bedindungen sind durch die Anwendung eines Einmal-Paßwort-Verfahrens bei den existierenden Filetransfer-Protokollen erfüllbar. Zum Schutz vor Replay-Attacken wird das Verfahren der Einweg-Verschlüsselung für die Filetransfer-Protokolle adaptiert. Die Generierung eines Einmal-Paßworts erfordert im allgemeinen Fall folgende Komponenten:

a) Ein symmetrischer Schlüssel (geheimes Paßwort), der nur beim Initiator (Client) und beim Server, der die Authentisierung durchführt, bekannt ist. Dieses Paßwort selbst wird nicht (unverschlüsselt) übertragen.

b) Ein Initiator ID zur eindeutigen Identifizierung des Initiators.

c) Variable Komponenten, wie Uhrzeit und/oder Zufallszahlen und/oder Folgenummern. Diese Komponenten ändern sich bei jeder Authentisierung und verhindern somit, daß ein abgehörtes Einmalpaßwort für eine Replay-Attacke wiederverwendet werden kann. Sofern diese Komponenten beim Server nicht automatisch abgeleitet werden können, müssen sie bei der Authentisierung mit übertragen werden.

d) Zusätzliche Daten, wie z.B. Initiator Id oder beliebiger Text, die in die Bildung des Einmal-Paßworts mit einfließen. Diese Daten sind entweder auf bei beiden Seiten bekannt bzw. ableitbar oder werden zusätzlich übertragen.

e) Eine codierte Information (Einmal-Paßwort), die mit Hilfe einer Einweg-Funktion zur Verschlüsselung aus obigen Kompo-

nenten in einem einstufigen Verfahren oder in einem mehrstufigen Verfahren - evtl. durch verschiedene Einweg-Funktionen - gebildet wird (siehe FIG 1).

Verfahren zur Einweg-Verschlüsselung und Authentisierung sind z.B. in ITU rec. X.509 (Directory Authentication - siehe 2.) und ISO 9798-4 dokumentiert.

Die Authentisierungs-Protokolle für Filetransfer sehen nur die Übertragung eines unstrukturierten Paßwortstrings vor und nicht die strukturierte Übertragung verschiedener Komponenten, wie dies bei der Verwendung von Einmal-Paßwörtern erforderlich wäre.

Um diesen Nachteil zu überwinden wird daher ein Verfahren eingeführt, das - transparent für das eigentliche Filetransfer-Protokoll - eine eindeutige Abbildung dieser Komponenten auf den Paßwortstring durchführt. Diese Abbildung muß beim Initiator und beim Server bekannt und identisch sein. Hierbei sind u.a. folgende Verfahren möglich:

- Die einzelnen Komponenten werden auf festen Bytepositionen übertragen und ggf. mit vorgegebenen Füllbytes aufgefüllt.
- Es werden zusätzlich Pointer auf die einzelnen Komponenten auf festen Positionen übertragen.
- Die Komponenten werden in einer festen Reihenfolge mit zusätzlichen Längenfeldern übertragen.

Diese Abbildung ist bei einem Kommunikations-Protokoll, das bezüglich der Sicherung des Zugangs nur die Übertragung eines unstrukturierten Paßwort-Strings vorsieht, z.B. bei FTAM/FTP, ohne Protokolländerung möglich. Die Codierung des Paßworts beim Initiator und die Verifikation im Server kann dabei durch zusätzliche Komponenten außerhalb des eigentlichen Filetransfer-Protokolls erfolgen. In den Fällen, in denen Paßwörter (z.B. FTP) nicht binär übertragbar sind, kann zusätz-

lich eine ASCII-Codierung - mit Hilfe eines gängigen Verfahrens - des Binärpaßworts vorgenommen werden.

Die Generierung des Einmal-Paßworts erfolgt in einem einstufigen Verfahren gemäß ITU rec. X.509; als Einweg-Funktion zur Paßwort-Verschlüsselung wird der MD5 (Message Digest) Algorithmus nach RFC 1325 verwendet. Die einzelnen Komponenten werden auf festen Bytepositionen im Paßwortstring übertragen (siehe FIG 2)

Neben der Implementierung der Initiator/Paßwort-Authentisierung im FTAM/FTP-Server im Netzelement ist eine entsprechende Funktion bei den FTAM-/FTP-Clients in den Bedienrechnern (OS) zur Generierung des Einmal-Paßworts erforderlich (siehe FIG 3).

Im folgenden werden anhand von FIG 3 nochmals die Schritte des Verfahrens erläutert:

1): Für die Authentisierung beim Aufbau einer FTAM/FTAM Verbindung wird die Initiator-Id und das zugehörige Paßwort übergeben.
2) + 3): Aus dem Paßwort generiert eine spezielle Generator-Komponente das strukturierte Einmalpaßwort bestehend aus Datum/Uhrzeit (time) und/oder Zufallszahl (random) und dem Ergebnis der Einwegverschlüsselung (rpPW).
4): Der FTAM/FTP client überträgt das strukturierte Einmalpaßwort und die Initiator-Id beim Verbindungsaufbau an den entfernten FTAM/FTP Server.
5): Die Authentisierungsinformation wird einer speziellen Komponente zur Verifikation übergeben.
6)+ 7): Aus der Authentisierungsdatenbasis wird das (geheime) Paßwort des Initiators ausgelesen. Mit diesem Paßwort wird die gleiche Einwegverschlüsselung wie beim Initiator durchgeführt. Die Authentisierung ist erfolgreich, wenn der hierbei generierte Wert identisch mit dem übertragenen rpPW ist.

7): Abhängig vom Ergebnis der Verifikation wird der Verbindungsaufbau akzeptiert oder abgelehnt.

Verwendete Abkürzungen:

| | |
|---|---|
| FTAM | File Transfer Access and Management |
| FTP | File Transfer Protocol |
| ITU | International Telecommunication Union |
| ISO | International Standardization Organization |
| MD5 | Message Digest Algorithmus No. 5 |
| MML | Man Machine Language |
| OWF | One Way Function |
| OS | Operations System |
| RFC | Request for Comment |
| TMN | Telecomunication Management Network |

Patentansprüche

1. Verfahren zur Sicherung des Zugangs zu einer Anwendung eines vernetzten Systems, wobei die Anwendung ein Kommunikations-Protokoll benutzt, das bezüglich der Zugangssicherung die Übertragung eines unstrukturierten Paßwort-Strings vorsieht, demgemäß

a) von einer Initiator-Komponente der Anwendung ein Einmal-Paßwort gebildet wird,

b) von der genannten Initiator-Komponente das strukturierte Einmal-Paßwort in den unstrukturierten Paßwort-String des Kommunikations-Protokolls abgebildet wird und mit Hilfe des gen. Kommunikations-Protokolls zu einer Reaktions-Komponente der Anwendung gesendet wird,

c) von der genannten Reaktions-Komponente aus dem empf Paßwort-String das darin abgebildete Einmal-Paßwort entnommen wird,

d) von der genannten Reaktions-Komponente nachfolgend anhand des Einmal-Paßwort eine Auth. des Initiators durchgeführt wird.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß
das Einmal-Paßwort in den unstrukturierten Paßwort-String abgebildet wird, indem die einzelnen Komponenten des Einmal-Paßwort auf festen Bytepositionen des Paßwort-Strings übertragen und ggf. mit vorgegebenen Füllbytes aufgefüllt werden.

3. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß
das Einmal-Paßwort in den unstrukturierten Paßwort-String abgebildet wird, indem Pointer auf festen Positionen des Paßwort-Strings übertragen werden, die auf die einzelnen Komponenten des Einmal-Paßwort innerhalb des Paßwort-Strings zeigen.

4. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß
das Einmal-Paßwort in den unstrukturierten Paßwort-String abgebildet wird, indem im Paßwort-String die Komponenten des Einmal-Paßwort in einer festen Reihenfolge übertragen werden, wobei jede Komponente ein zusätzliches Längenfeld umfaßt.

5. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet, daß
es sich bei dem genannten Kommunikations-Protokoll um FTAM nach ISO 8571 oder FTP nach RFC 959 u. RFC 1123 handelt.

6. Anwendungssystem eines vernetzten Systems, mit
a) einem Kommunikations-Protokoll, das bezüglich der Sicherung des Zugangs die Übertragung eines unstrukturierten Paßwort-Strings vorsieht,
b) einer Initiator-Komponente, die die Anwendung initiiert, indem sie eine Verbindungsanforderungs-Nachricht zu einer Reaktions-Komponente sendet, die den genannten unstrukturierten Paßwort-String enthält,
c) einer Reaktions-Komponente, die genannte Verbindungsanforderungs-Nachricht bearbeitet, wobei sie hierbei anhand des Paßwort-Strings eine Authenzitätsprüfung durchführt,
dadurch gekennzeichnet, daß
d) die Initiator-Komponente das Paßwort in einer eindeutigen Weise auf das Paßwort abbildet,
e) die Initiator-Komponente den derart vorbereiteten Paßwort-String mithilfe des gen. Kommunikations-Protokolls zur Reaktions-Komponente sendet,
f) die Reaktions-Komponente dem empf Paßwort-String das darin abgebildete Einmal-Paßwort entnimmt,
g) die Reaktions-Komponente nachfolgend anhand des Einmal-Paßworts eine Auth. des Initiators durchführt.

7. Anwendungssystem nach Anspruch 6,
dadurch gekennzeichnet, daß

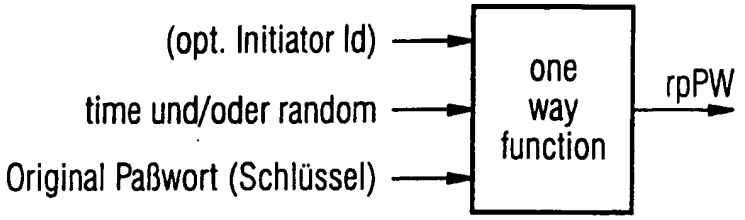
es sich bei dem Anwendungssystem um ein File-Transfer-System handelt.

8. Initiator-Komponente eines Anwendungssystems für eine verteilte Anwendung, mit
a) einer Client-Komponente, die die Anwendung initiiert, indem sie eine Verbindungsanforderungs-Nachricht zu einer Reaktions-Komponente sendet, die einen unstrukturierten Paßwort-String enthält,
gekennzeichnet durch
b) eine Generator-Komponente, die ein strukturiertes Einmal-Paßwort generiert und das strukturierte Einmal-Paßwort in den unstrukturierten Paßwort-String der Client-Komponente abbildet.

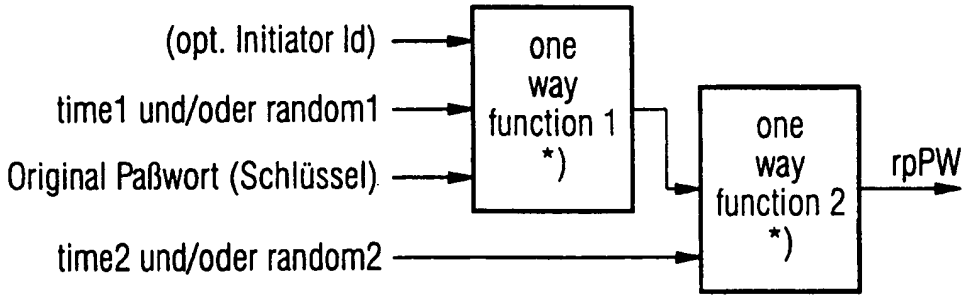
9. Reaktions-Komponente eines Anwendungssystems für eine verteilte Anwendung, mit
einer Server-K, die eine Verbindungsanforderungs-Nachricht bearbeitet, wobei sie hierbei den in der Verbindungsanforderungs-Nachricht enthaltenen Paßwort-String an eine Auth.-Komponente übergibt,
gekennzeichnet durch
die genannte Auth.-Komponente, die aus dem empf Paßwort-String das darin abgebildete Einmal-Paßwort entnimmt und nachfolgend anhand des Einmal-Paßworts eine Auth. des Initiators durchführt.

**FIG 1** Generierung der Komponente rpPaßwort eines Einmal-Paßworts nach ITU rec. X.509

1. Einstufige Paßwort-Verschlüsselung

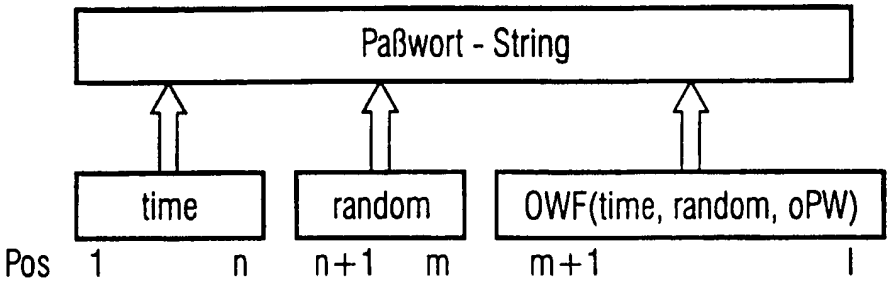



2. Zweistufige Paßwort-Verschlüsselung




*) Beide Funktionen können identisch sein

**FIG 2** Übertragung des Einmal-Paßworts im Paßwortstring




OWF=one way function

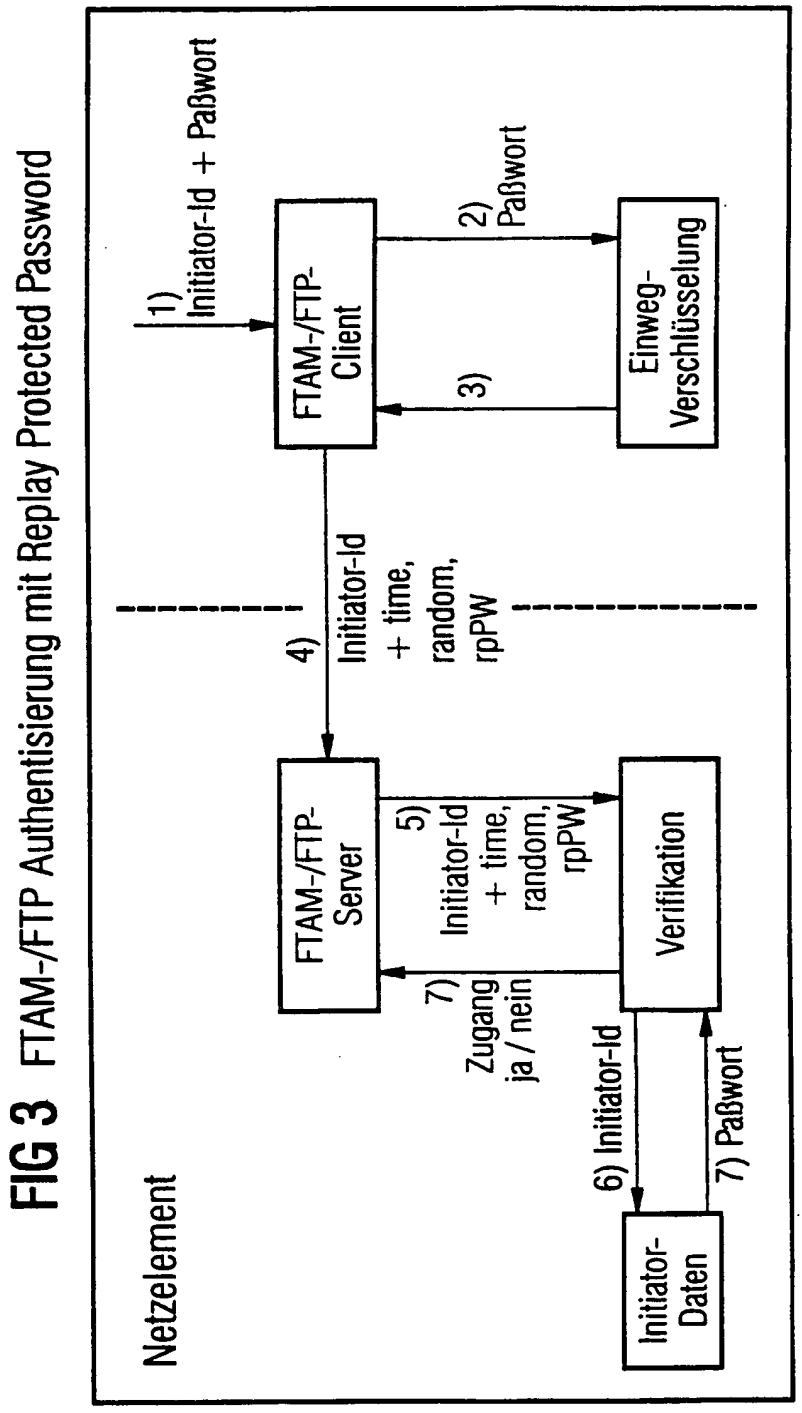



FIG 3 FTAM-/FTP Authentisierung mit Replay Protected Password

# INTERNATIONAL SEARCH REPORT

Inte ,onal Application No
PCT/EP 98/06211

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/22 H04L29/06 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 5 661 807 A (GUSKI RICHARD HENRY ET AL) 26 August 1997<br>see column 1, line 6 - column 3, line 8<br>see column 3, line 16 - line 58<br>see column 6, line 6 - column 7, line 3<br>see column 7, line 45 - column 10, line 21<br>see column 11, line 5 - column 14, line 35<br>see figure 3 | 1-9 |
| A | EP 0 686 905 A (SUN MICROSYSTEMS INC) 13 December 1995<br>see page 3, column 2, line 6 - line 40 | 5,7 |
| A | EP 0 349 464 A (IBM) 3 January 1990<br>see page 2, column 2, line 19 - line 32<br>see page 2, column 2, line 61 - page 3, column 3, line 22; figure 1 | 3 |

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 15 February 1999 | 23/02/1999 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Karavassilis, N |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Inte .onal Application No
PCT/EP 98/06211

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 4 924 515 A (MATYAS STEPHEN M ET AL) 8 May 1990 see column 14, line 35 - column 15, line 33 see column 17, line 62 - column 18, line 6; figures 15,17 --- | 4 |
| A | EP 0 774 707 A (BULL SA) 21 May 1997 ----- | |

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/EP 98/06211

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 5661807 A | 26-08-1997 | EP 0636963 A | 01-02-1995 |
| | | JP 7107086 A | 21-04-1995 |
| | | US 5592553 A | 07-01-1997 |
| EP 0686905 A | 13-12-1995 | US 5604803 A | 18-02-1997 |
| | | JP 8227397 A | 03-09-1996 |
| | | US 5732137 A | 24-03-1998 |
| EP 0349464 A | 03-01-1990 | US 5214779 A | 25-05-1993 |
| | | JP 2046049 A | 15-02-1990 |
| US 4924515 A | 08-05-1990 | CA 1319198 A | 15-06-1993 |
| | | DE 68926005 D | 25-04-1996 |
| | | DE 68926005 T | 17-10-1996 |
| | | DE 68926076 D | 02-05-1996 |
| | | DE 68926076 T | 14-11-1996 |
| | | EP 0356065 A | 28-02-1990 |
| | | EP 0354770 A | 14-02-1990 |
| | | JP 2096841 C | 02-10-1996 |
| | | JP 2106787 A | 18-04-1990 |
| | | JP 8016825 B | 21-02-1996 |
| EP 0774707 A | 21-05-1997 | FR 2741465 A | 23-05-1997 |
| | | CA 2190690 A | 21-05-1997 |
| | | US 5841871 A | 24-11-1998 |

# - INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 98/06211

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**
IPK 6 H04L12/22 H04L29/06 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole )
IPK 6 H04L G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| X | US 5 661 807 A (GUSKI RICHARD HENRY ET AL) 26. August 1997<br>siehe Spalte 1, Zeile 6 - Spalte 3, Zeile 8<br>siehe Spalte 3, Zeile 16 - Zeile 58<br>siehe Spalte 6, Zeile 6 - Spalte 7, Zeile 3<br>siehe Spalte 7, Zeile 45 - Spalte 10, Zeile 21<br>siehe Spalte 11, Zeile 5 - Spalte 14, Zeile 35<br>siehe Abbildung 3<br>--- | 1-9 |
| A | EP 0 686 905 A (SUN MICROSYSTEMS INC) 13. Dezember 1995<br>siehe Seite 3, Spalte 2, Zeile 6 - Zeile 40<br>---<br>-/-- | 5,7 |

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

| Datum des Abschlusses der internationalen Recherche | Absendedatum des internationalen Recherchenberichts |
|---|---|
| 15. Februar 1999 | 23/02/1999 |

| Name und Postanschrift der Internationalen Recherchenbehörde | Bevollmächtigter Bediensteter |
|---|---|
| Europäisches Patentamt, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Karavassilis, N |

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

# INTERNATIONALER RECHERCHENBERICHT

Inte onales Aktenzeichen
PCT/EP 98/06211

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| A | EP 0 349 464 A (IBM) 3. Januar 1990<br>siehe Seite 2, Spalte 2, Zeile 19 - Zeile 32<br>siehe Seite 2, Spalte 2, Zeile 61 - Seite 3, Spalte 3, Zeile 22; Abbildung 1 | 3 |
| A | US 4 924 515 A (MATYAS STEPHEN M ET AL) 8. Mai 1990<br>siehe Spalte 14, Zeile 35 - Spalte 15, Zeile 33<br>siehe Spalte 17, Zeile 62 - Spalte 18, Zeile 6; Abbildungen 15,17 | 4 |
| A | EP 0 774 707 A (BULL SA) 21. Mai 1997 | |

1

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 98/06211

| Im Recherchenbericht angeführtes Patentdokument | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | Datum der Veröffentlichung |
|---|---|---|---|
| US 5661807 A | 26-08-1997 | EP 0636963 A | 01-02-1995 |
| | | JP 7107086 A | 21-04-1995 |
| | | US 5592553 A | 07-01-1997 |
| EP 0686905 A | 13-12-1995 | US 5604803 A | 18-02-1997 |
| | | JP 8227397 A | 03-09-1996 |
| | | US 5732137 A | 24-03-1998 |
| EP 0349464 A | 03-01-1990 | US 5214779 A | 25-05-1993 |
| | | JP 2046049 A | 15-02-1990 |
| US 4924515 A | 08-05-1990 | CA 1319198 A | 15-06-1993 |
| | | DE 68926005 D | 25-04-1996 |
| | | DE 68926005 T | 17-10-1996 |
| | | DE 68926076 D | 02-05-1996 |
| | | DE 68926076 T | 14-11-1996 |
| | | EP 0356065 A | 28-02-1990 |
| | | EP 0354770 A | 14-02-1990 |
| | | JP 2096841 C | 02-10-1996 |
| | | JP 2106787 A | 18-04-1990 |
| | | JP 8016825 B | 21-02-1996 |
| EP 0774707 A | 21-05-1997 | FR 2741465 A | 23-05-1997 |
| | | CA 2190690 A | 21-05-1997 |
| | | US 5841871 A | 24-11-1998 |